

Is Microsoft 365 Email Security Good Enough to Prevent a Cyber Attack?

Basic Email Security is not Enough.

- » The majority of cyber attacks start with email. According to research by Egress – 94% of malware is communicated via email.
- » Protecting your business from malware, spam, and BEC attacks requires more than just basic email security.

Why you need SpamTitan if you're relying on Microsoft Defender?

Some key reasons why organizations choose to augment Microsoft Defender with a third-party email security solution:

1. Specialized Email Protection

Third-party email security solutions are specifically designed to address the unique challenges of email security, such as phishing attacks, spam, malware, and email fraud. They provide advanced filtering and scanning capabilities to detect and block email-based threats.

2. Additional Layers of Defense

Every hacker has a keen interest in M365. Layered security is the best cybersecurity practice. Using a third-party solution adds an extra layer of protection to your email infrastructure. This can help catch threats that may bypass Microsoft Defender. No one technology provides security for everything; that's why different layers are crucial. Relying on a single vendor for all your security needs can be risky.

3. Advanced Threat Detection

Third-party solutions often employ more advanced threat detection techniques, including machine learning and artificial intelligence, to identify evolving and sophisticated email threats.

4. False Positives & False Negatives

Microsoft 365 Defender generates false positive alerts, which can lead to security teams spending time investigating non-existent threats. This can be frustrating and time-consuming. On the flip side, the solution does not always detect security threats, allowing some malicious activity to go unnoticed.

5. Cost Reduction

The cost of basic M365 is \$11.70 pupm and the upgrade to premium M365 with advanced security is \$20.60 pupm – that's a staggering jump of \$8.90 pupm for a service you may not need. *SpamTitan offers more advanced protection for \$2.75 pupm. *based on 1 year subscription.

“

Every hacker has a keen interest in M365.

”

6. Zero-Day Protection

Email security solutions may provide zero-day threat protection by identifying and blocking new, previously unknown threats, while Microsoft Defender may require updates to recognize them.

7. Customization and Policies

Many third-party solutions offer extensive customization and policy options for organizations to define and enforce specific security rules and configurations tailored to their needs.

8. Increased Accuracy

Specialized email security solutions often have lower false-positive rates, reducing the chances of legitimate emails being classified as spam or blocked.

9. Reporting and Compliance

SpamTitan provides comprehensive reporting and analytics, making tracking and analyzing email and security incidents easier. Administrators love the easy-to-use admin tools SpamTitan offers versus a non-user-friendly MS alternative.

10. Centralized Management

Integrating a third-party solution into your email ecosystem can provide centralized management and monitoring capabilities for your email security, making it more efficient to oversee email security across the organization.

11. Scalability and Performance

Some third-party solutions are highly scalable and can handle a large volume of email traffic without affecting performance, which is essential for organizations with high email traffic.

With SpamTitan, there are **fewer misses, fewer false positives, and less spam**, including malicious emails containing malware. No single technology provides security for everything; that's why different layers are crucial. Relying on a single vendor for all your security needs can be risky.

